UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,899	11/24/2001	Helge Bragstad	40.0043	7679

41754 7590 08/24/2005

PEHR JANSSON, ATTORNEY AT LAW
7628 PARKVIEW CIRCLE
AUSTIN, TX 78731

EXAMINER
KHOSHNOODI, NADIA

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 08/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/993,899	BRAGSTAD ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11/24/2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/5-27-2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

The disclosure is objected to because of the following informalities: A summary of the invention has not been included. See MPEP 608.01[R-2]. Appropriate correction is required.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teppler, US Patent No. 6,792,536 and further in view of Chandersekaran et al., US Patent No. 6,335,972.

As per claims 1, 10, 19:

Teppler substantially teaches a method, computer program product, and apparatus for accessing cryptographic material comprising the steps of: creating cryptographic material, by a first Cryptographic-related application programming interface ("API"), in response to a request by a first application compatible with the first Cryptographic-related API (col. 33, lines 6-34).

Not explicitly disclosed is creating a supplemental aspect of the cryptographic material by a supplemental method for the first cryptographic API, wherein the supplemental aspect includes information for rendering the cryptographic material compatible with a second Cryptographic-related API so that the cryptographic material is accessible for a second application by the second Cryptographic-related API. However, Chandersekaran et al. teach a key recovery API that is compatible with the Cryptographic-related API in order to gain access

to the cryptographic material if necessary. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Teppler for the supplemental aspect to include information for rendering the cryptographic material compatible with a second Cryptographic-related API so that the cryptographic material is accessible for a second application by the second Cryptographic-related API. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Chandersekaran et al. in col. 13, lines 21-43.

As per claim 2, 11, and 20:

Teppler and Chandersekaran et al. substantially teach the method, computer program product, and apparatus of claims 1, 10, and 19. Furthermore, Teppler teaches wherein the step of creating cryptographic material comprises creating a certificate or private key (col. 33, lines 6-20). Not explicitly disclosed is the step of creating the supplemental aspect of the cryptographic material comprises the steps of: deriving a key container name from the certificate or private key; and determining whether the key container already exists. However, Chandersekaran et al. teach generating key recovery fields where if the recovery field exists these fields may be updated. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Teppler for the supplemental aspect to include deriving a key container name from the certificate or private key; and determining whether the key container already exists. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Chandersekaran et al. in col. 15, line 49 – col. 16, line 31.

As per claim 3, 12, and 21:

Teppler and Chandersekaran et al. substantially teach the method, computer program product, and apparatus of claims 2, 11, and 20. Furthermore, Teppler teaches wherein the step of deriving a key container name comprises the steps of: creating a hash responsive to material from the certificate or private key; and encoding the hash (col. 33, lines 35-56).

As per claims 4, 13, and 22:

Teppler and Chandersekaran et al. substantially teach the method, computer program product, and apparatus of claims 2, 11, and 20. Furthermore, Teppler teaches wherein the step of creating a certificate or private key comprises creating the private key (col. 33, lines 6-20). Not explicitly disclosed is wherein if the key container already exists for the key, the step of creating the supplemental aspect of the cryptographic material comprises the steps of: determining whether the key container contains a certificate; associating the private key as a member of a key pair associated with the certificate, if the key container contains a certificate; and associating the private key as a member of a key pair having a default key specification, if the key container does not contain a certificate. However, Chandersekaran et al. teach creating various key recovery fields for keys that exist as well as having a certificate and key recovery contexts for the key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Teppler to creating the supplemental aspect of the cryptographic material comprises the steps of: determining whether the key container contains a certificate; associating the private key as a member of a key pair associated with the certificate, if the key container contains a certificate; and associating the private key as a member of a key pair having a default key specification, if the key container does not contain a certificate. This

modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Chandersekaran et al. in col. 17, lines 17-36 and col. 18, lines 1-9.

As per claims 5, 14, and 23:

Teppler and Chandersekaran et al. substantially teach the method, computer program product, and apparatus of claims 2, 11, and 20. Furthermore, Teppler teaches wherein the step of creating a certificate or private key comprises creating the certificate (col. 33, lines 6-20). Not explicitly disclosed is the step of creating the supplemental aspect of the cryptographic material comprises the steps of extracting a key specification from the certificate and associating the certificate with a key pair under the extracted key specification. However, Chandersekaran et al. teach that a profile is created which creates an association with the various certificate chains corresponding to a key pair. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Teppler for creating the supplemental aspect of the cryptographic material to comprise the steps of extracting a key specification from the certificate and associating the certificate with a key pair under the extracted key specification. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Chandersekaran et al. in col. 17, line 54 - col. 18, line 9.

As per claims 6, 15, and 24:

Teppler and Chandersekaran et al. substantially teach the method, computer program product, and apparatus of claims 2, 11, and 20. Furthermore, Teppler teaches wherein the step of creating a certificate or private key comprises creating the certificate (col. 33, lines 6-20). Not

explicitly disclosed is wherein if the key container already exists for the certificate the step of creating the supplemental aspect of the cryptographic material comprises the steps of: determining whether the key container has a private key; and associating the private key with a same key pair as the certificate, if the key container has the private key. However, Chandersekaran et al. teach a profile connected to a key where the key is associated with the certificate chain for the user. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Teppler for the certificate the step of creating the supplemental aspect of the cryptographic material comprises the steps of: determining whether the key container has a private key; and associating the private key with a same key pair as the certificate, if the key container has the private key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Chandersekaran et al. in col. 17, line 54 - col. 18, line 9.

As per claims 7, 16, and 25:

Teppler and Chandersekaran et al. substantially teach the method, computer program product, and apparatus of claims 2, 11, and 20. Furthermore, Teppler teaches wherein the step of creating a certificate or private key comprises creating the certificate (col. 33, lines 6-20). Not explicitly disclosed is the step of creating the supplemental aspect of the cryptographic material comprises the step of: creating a public key from information in the certificate. However, Chandersekaran et al. teaches that a public key certificate chain is comprised in the profile for the key recovery system. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Teppler for the step of creating the

supplemental aspect of the cryptographic material comprises the step of: creating a public key from information in the certificate. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Chandersekaran et al. in col. 17, line 54 - col. 18, line 9.

As per claims 8, 17, and 26:

Teppler and Chandersekaran et al. substantially teach the method, computer program product, and apparatus of claim 1, 10, and 19. Furthermore, Chandersekaran teaches wherein the first Cryptographic-related API is one from the set of PKCS #11, CryptoAPI, and CDSA compatible API's, and the second Cryptographic-related API is not the same API as the first and is also one from the set of PKCS #11, CryptoAPI and CDSA compatible API's (col. 10, lines 1-49).

As per claims 9, 18, and 27:

Teppler and Chandersekaran et al. substantially teach the method, computer program product, and apparatus of claims 1, 10, and 19. Furthermore, Chandersekaran et al. teach wherein the first Cryptographic-related API uses a certain term and the second Cryptographic-related API has a corresponding term, and wherein creating the supplemental aspect comprises creating material indicating a cross-reference between the term (col. 11, lines 7-64).

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,385,729
2. US Patent No. 6,772,341

3. US Patent No. 6,484,259
4. US Patent No. 5,996,076

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JOSEPH TORRES
PRIMARY EXAMINER

Nadia Khoshnoodi
Examiner
Art Unit 2133
8/16/2005

NK